A Novel Approach For Current Scenario In New Development For Automated Network Defense System

Synopsis submitted to IIMT University in the partial fulfillment

of the requirement for the award of the degree of

DOCTOR OF PHILOSOPHY

In

Computer Science and Applications

By

Brajesh Raj

Admission No. 21211399

Part Time

Under the Guidance of

Dr. Kewal Krishan Sharma

Professor, School of Computer Science and Applications

IIMT UNIVERSITY MEERUT
Transforming Education System, Transforming Lives

UGC Approved
Section 2(f) & 12B

School of Computer Science and Applications

IIMT University, Meerut

Year-2022-23

Dean
School of Computer Scie
IIMT University, Meerut (UP)

TABLE OF CONTENTS

S. No.	Particular	Page No.
1	Introduction	3
2	Literature survey	5
3	Research Gap	8
4	Research objectives	8
5	Proposed Methodology	8
6	Research Tools and Techniques	10
7	Expected Outcome	10
8	Conclusion	11
9	References	11

1. Introduction

The digital landscape is continuously evolving, becoming increasingly complex and interconnected, while simultaneously facing a surge in sophisticated cyber threats. Traditional network defense mechanisms, often reliant on static signatures and manual intervention, are proving inadequate against dynamic and persistent attacks, particularly Advanced Persistent Threats (APTs) and zero-day exploits. This critical vulnerability highlights the urgent need for a paradigm shift toward intelligent, autonomous systems that can proactively defend against threats. This synopsis proposes a novel approach for developing an Automated Network Defense System that leverages cutting-edge artificial intelligence, specifically reinforcement learning, to address contemporary challenges.

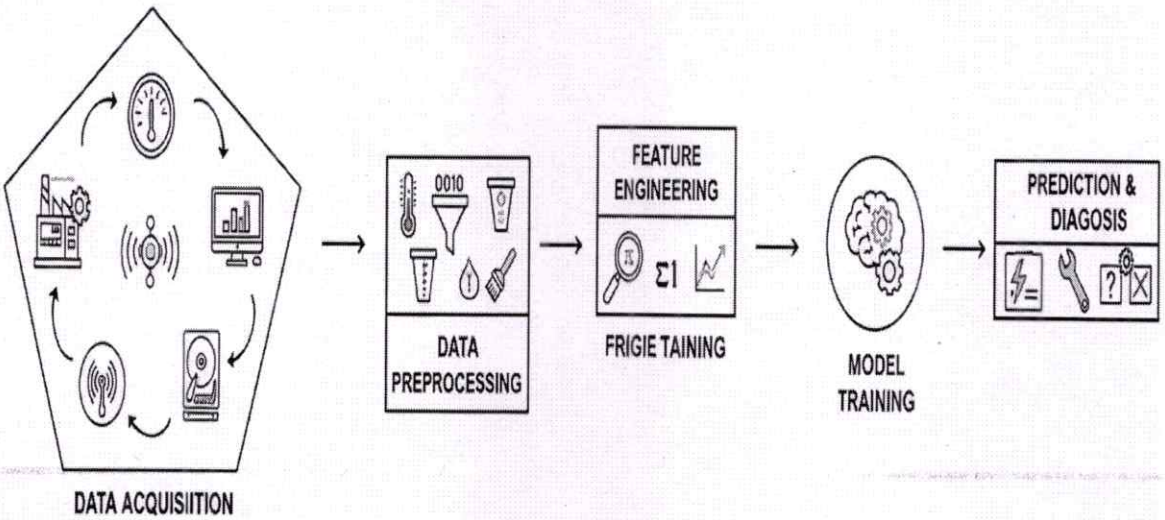

Figure 1: Data-driven Approach to Predictive Maintenance

This figure illustrates a typical workflow for a data-driven system, likely in the context of machine learning or data analysis. Let's break down the different stages:

Data Acquisition: This initial stage, represented by the pentagon on the left, shows various sources where data is collected. The icons suggest a diverse range, including what appears to be industrial equipment (factory/gear), environmental sensors (thermometer), network signals (Wi-Fi), data storage (hard drive), and possibly a computer or control panel. This stage emphasizes the collection of raw information from various points within a system or environment.

Data Preprocessing: Moving to the right, the next box signifies "Data Preprocessing." This crucial step involves cleaning, transforming, and organizing the raw data that has been collected. The icons within this box (thermometer, funnel, water drop, and binary code) hint at tasks like handling missing values, normalizing data, converting formats, and preparing it for analysis. The "0010" likely represents the digitized and structured nature of the data after this stage.

Feature Engineering: Following preprocessing is "Feature Engineering," a key step in machine learning. This involves selecting, creating, and transforming raw features into variables that are more informative and suitable for model training. The icons here (magnifying glass, sigma, and a graph/chart) suggest statistical analysis, aggregation, and the extraction of relevant patterns or characteristics from the data.

Model Training: The "Model Training" stage, depicted by a brain icon with gears, represents the core of machine learning, where an algorithm learns from the engineered features. The brain symbolizes artificial intelligence or a learning algorithm, and the gears indicate the computational process involved in building and optimizing the model.

Prediction & Diagnosis: The final stage is "Prediction & Diagnosis." Here, the trained model is used to make predictions or diagnose issues. The icons (lightning bolt, wrench, question mark, and checkmark/X /X) suggest various outcomes:

Lightning bolt: Perhaps indicating an event detection or an alert.

Wrench: Suggesting a repair or maintenance action.

Question mark: Representing a query, uncertainty, or a need for further investigation.

Checkmark/X /X: Denoting a decision, classification, or the outcome of a diagnostic test (e.g., regular vs. anomaly). The proposed system is designed not only to detect and mitigate threats in real-time autonomously but also to be inherently robust against attacks targeting its own AI core and adaptable to novel, unseen attack scenarios. This introduction establishes the pressing necessity for such innovation and outlines the framework for a more resilient and intelligent future for cybersecurity.

2. Literature Reviews

The escalating sophistication and volume of cyber threats have rendered traditional, static defense mechanisms increasingly obsolete. This has catalyzed a paradigm shift towards Autonomous Cyber Defense (ACD) systems, which leverage artificial intelligence (AI) to detect, analyze, and counter threats in real-time dynamically. This literature review synthesizes current research on ACD, with a focus on reinforcement learning (RL) applications, simulation environments, multi-agent strategies, and the critical challenges of explainability and security [1],[19].

1. The Evolution Towards Autonomous Cyber Defense

The foundational shift towards automation is well documented. Vyas, Hannay, Bolton, and Burnap provide a comprehensive review of automated cyber defense [13], emphasizing the urgent requirement for systems capable of operating at machine speeds to address contemporary cyber threats. Vyas, Mavroudis, and Burnap extend this analysis by systematically reviewing the deployment of autonomous agents in real-world environments [14]. Their work highlights the progression from theoretical models to practical implementations and identifies significant technical and operational challenges. Kott suggested, this perspective by introducing the Autonomous Intelligent Cyber Defense Agent (AICA) framework, which defines the core architectural principles for proactive and adaptive cyber defense systems [6].

2. Reinforcement Learning as a Core Paradigm

Reinforcement Learning has emerged as a primary engine for ACD due to its ability to learn optimal policies through environmental interaction. A significant challenge in this domain is designing effective reward structures. Bates, Mavroudis, and Hicks investigate reward shaping techniques to accelerate the training of RL agents and improve policy stability, moving beyond simple, sparse rewards. However, the safety of the RL training process is a critical concern [1]. BHARTI et al. and Cui et al. addressed the threat of backdoor attacks, where an opponent manipulates the training process to create hidden vulnerabilities [2], [3]. BHARTI et al. Proposed a proven defense against these policies [2], while cui et al. Demonstrate a sparse and directed attack by Backdoor (Badrl), highlighting the fragility of RL models [3]. Complementing this, Guo et al. "Polycyclean" gift, a method for explicitly designed backdoor detection and mitigation for competitive reinforcement learning environments [4].

3. Simulation and Training Environments

Training reliable RL agents requires robust, scalable simulation environments. Janisch, Pevný, and Lisý introduce NASimEmu, a combined simulator and emulator designed to train agents that can generalize to novel network scenarios, thereby addressing the problem of overfitting to specific training conditions [5]. The theoretical underpinnings of decision-making in these environments are often based on control theory. Kappen provides the foundational work on optimal control theory and the linear Bellman equation, which forms the mathematical basis for many RL algorithms used in ACD [7].

4. Game-Theoretic and Multi-Agent Defense Strategies

Cyber defense constitutes a multi-agent, adversarial challenge. Game theory offers a rigorous framework for analyzing these interactions. Yang et al. and Zhang et al. employed game-theoretic models to examine conflicts between attackers and defenders, with a focus on critical infrastructure protection and remote state estimation [21], [24]. Mejdi and Ezzedine introduce dynamic defense strategies for networked control systems subject to stochastic jamming attacks, emphasizing the importance of adaptive response mechanisms [8]. Wang et al. extend this work by applying a Bayesian Stackelberg game model to remote state estimation in systems with arbitrary tree topologies under Denial-of-Service (DoS) attacks [15]. In distributed environments such as fog computing, Waqas et al. design a defense scheme targeting Advanced Persistent Threats (APTs), underscoring the necessity for decentralized defensive coordination [16].

5. Detection of Advanced Persistent Threats (APTs)

APTs represent a particularly sophisticated class of threats requiring specialized detection methods. Several researchers have proposed novel machine learning-based approaches. Xuan and Dao and Xuan, Duong, and Dau developed combined deep learning models and multi-layer traffic analysis techniques, respectively, for APT detection [17], [18]. More recently, Xuan and Nguyen advanced this field with a novel approach based on "advanced computing." Similarly, Sharma et al. proposed a multi-dimensional hybrid Bayesian belief network for APT malware detection [12], [19], while Xue et al. designed a detection scheme based on CK sketch and DNS traffic analysis [20].

6. Explainability and Regulatory Governance

As ACD systems grow more complex, their "black-box" nature becomes a barrier to trust and adoption. Dazeley, Vamplew, and Cruz survey this critical issue, proposing a conceptual framework for Explainable AI (XAI) in reinforcement learning ("Broad-XAI") to make autonomous decisions more interpretable to human analysts. Concurrently, the rapid deployment of AI in security necessitates robust governance [10]. Devitt and Copeland analyze Australia's approach to AI governance in security and defence, reflecting a growing global focus on the ethical and regulatory frameworks required for autonomous systems [11].

7. Optimization and Control in Networked Systems

The practical implementation of ACD relies on sophisticated optimization techniques. Ponce-Ortega, Ochoa-Barragán, and Ramírez-Márquez discuss the use of software like MATLAB for optimization in complex systems, which is directly applicable to tuning ACD parameters [9]. Furthermore, Yu et al. and Zhou, Shang, and Chen address the challenges of maintaining control and security in networked systems [23], [25], with Yu et al. focusing on optimal resilient tracking control under attacks [23] and Zhou et al. providing a comprehensive review of cybersecurity for remote state estimation [25].

3. Research Gap

The current literature demonstrates significant progress in individual components of ACD: RL training, secure learning, game theory, APT detection, and simulation. However, a gap exists in the integrated development of a secure, explainable, and generalizable RL-based defense framework. Many studies address these challenges in isolation (e.g., security OR explainability OR generalization) [3]. While significant progress has been made in developing autonomous cyber defense (ACD) systems using reinforcement learning (RL), current research often addresses the challenges of security, generalizability, and explainability in isolation [4]. A critical gap exists in the integrated development of an RL-based defense framework that is simultaneously robust against training-phase adversarial attacks (e.g., backdoor policies), capable of generalizing to novel network topologies and threat scenarios, and inherently explainable to facilitate human trust and operational deployment. This research aims to fill this gap by proposing a new ACD approach that synthesizes these three critical dimensions in a unified, resilient, and reliable self-employed

defense system. The proposed system will be validated against current APT detection references to demonstrate a holistic advance in the automated defense of the network [22].

4. Research Objectives

This research aims to design a reinforcement learning-based architecture for automated network defense, enabling real-time threat detection and mitigation. The project will prioritize strengthening the system's security and robustness by incorporating defenses against adversarial attacks, including backdoor poisoning [1]. The proposed system will be rigorously evaluated in a simulated environment and benchmarked against state-of-the-art solutions, using metrics such as detection accuracy, response time, and adaptability to new attack vectors [8],[9].

- **To design a novel reinforcement learning-based architecture** for an automated network defense system that can autonomously detect and mitigate cyber threats.
- **To enhance the security and robustness** of the system by integrating mechanisms that defend against adversarial attacks targeting the AI model itself, such as backdoor poisoning during training.
- **To evaluate the performance** of the proposed system against current state-of-the-art solutions in a simulated environment, measuring key metrics such as detection accuracy, response time, and adaptability to novel attack vectors.

5. Proposed Methodology

The methodology will follow a structured, four-phase approach:

1. **Design and Development:** We will design a novel reinforcement learning architecture and use a simulated network environment for training. Adversarial training techniques will be applied to improve robustness against backdoor and poisoning attacks.
2. **Implementation and Training:** The RL agent will be implemented in a Python-based framework and trained on various attack scenarios, including advanced persistent threats and zero-day exploits, to develop effective defense policies.

3. **Testing and Evaluation:** The trained model will be rigorously tested against unseen attack vectors within the simulation environment. Its performance will be quantitatively evaluated and compared to baseline models using key metrics such as detection accuracy, false positive rate, mean time to response (MTTR), and system resilience.
4. **Analysis and Validation:** The results will be analyzed to assess the effectiveness, generalizability, and security of the proposed approach. The model's decision-making process will be validated for explainability to ensure its actions are interpretable by human analysts.

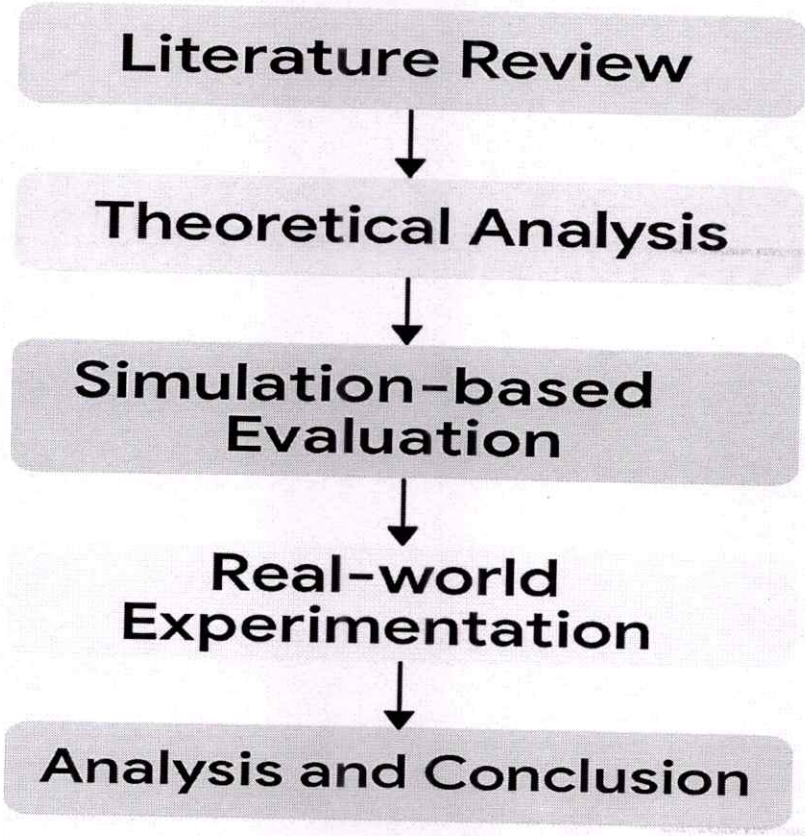

Figure 2: Proposed Methodology

6. Research Tools and Techniques

- **Simulation Environment:** NASimEmu or CyGym will be utilized as the primary platform to emulate complex network topologies and generate a wide array of cyber-attack scenarios for training and testing.
- **Development Frameworks:** Python will serve as the core programming language, leveraging AI libraries such as TensorFlow, PyTorch, and the OpenAI Gym interface for developing and training the reinforcement learning agents.
- **Modeling Techniques:** Deep Q-Networks (DQN) or Proximal Policy Optimization (PPO) algorithms will form the basis of the autonomous agent, potentially extended to a Multi-Agent RL (MARL) setting. Adversarial training techniques will be employed to enhance model robustness.
- **Data Analysis Tools:** MATLAB and specialized Python libraries (e.g., Scikit-learn, Pandas, NumPy) will be used for data preprocessing, statistical analysis, performance metric calculation, and visualization of results.

7. Expected Outcome

This research is expected to yield several key outcomes:

- A fully functional prototype of a novel, robust autonomous network defense system powered by a secure reinforcement learning algorithm.
- Empirical evidence indicates that the system outperforms existing solutions, as demonstrated by higher detection rates, fewer false positives, and faster response times to novel and advanced cyber threats.
- A comprehensive framework and set of design principles for developing explainable and attack-resistant AI models suitable for critical cybersecurity applications, contributing valuable knowledge to the field of automated cyber defense.

8. Conclusion

This synopsis has outlined a comprehensive research plan to address a critical and timely challenge at the intersection of cybersecurity. The escalating complexity of cyber threats necessitates a paradigm shift from traditional, static defense mechanisms towards intelligent, autonomous systems. This research proposal has outlined a novel approach for developing an automated network defense system that leverages advanced reinforcement learning to address critical challenges in the current landscape. By focusing on the integration of robustness against adversarial attacks, adaptability to novel scenarios, and operational explainability, the proposed system aims to enhance cyber resilience significantly. The successful execution of this research is expected to yield a validated prototype and contribute a valuable framework for the next generation of autonomous cybersecurity solutions, ultimately helping to protect critical digital infrastructure from evolving threats.

References:

[1]. Bates, E., Mavroudis, V., & Hicks, C. (2023). Reward shaping for happier, autonomous cybersecurity agents. *Proceedings of the 16th ACM Workshop on Artificial Intelligence and Security*, 221–232.

[2]. Bharti, S., Zhang, X., Singla, A., & Zhu, J. (2022). Provable defense against backdoor policies in reinforcement learning. *Advances in Neural Information Processing Systems, 35,* 14704–14714.

[3]. Cui, J., Han, Y., Ma, Y., Jiao, J., & Zhang, J. (2024). BadRL: Sparse targeted backdoor attack against reinforcement learning. *Proceedings of the AAAI Conference on Artificial Intelligence, 38,* 11687–11694.

[4]. J. Guo, A. Li, L. Wang and C. Liu, "PolicyCleanse: Backdoor Detection and Mitigation for Competitive Reinforcement Learning," *2023 IEEE/CVF International Conference on Computer Vision (ICCV)*, Paris, France, 2023, pp. 4676-4685, doi: 10.1109/ICCV51070.2023.00433.

[5]. Janisch, J., Pevný, T., Lisý, V. (2024). NASimEmu: Network Attack Simulator & Emulator for Training Agents Generalizing to Novel Scenarios. In: Katsikas, S., *et al.* Computer Security. ESORICS 2023 International Workshops. ESORICS 2023. Lecture Notes in Computer Science, vol 14399. Springer, Cham. https://doi.org/10.1007/978-3-031-54129-2_35

[6]. Kott, A. (2023). *Autonomous intelligent cyber defense agent (aica)*. Adelphi, MD, USA: Springer.

[7]. Kappen, H. J. (2011). *Optimal control theory and the linear Bellman equation*. Imperial College London. https://www.ma.imperial.ac.uk/~nsjones/timeseriesbook.pdf

[8]. Mejdi, H., & Ezzedine, T. (2024). Novel dynamic defense strategies in networked control systems under stochastic jamming attacks. *Mathematics, 12*(13), 2143. https://doi.org/10.3390/math12132143

[9]. Ponce-Ortega, J. M., Ochoa-Barragán, R., & Ramírez-Márquez, C. (2024). Optimization using the software MATLAB. In *Optimization of chemical processes: A sustainable perspective* (pp. 439–463). Springer Nature.

[10]. Richard Dazeley, Peter Vamplew, and Francisco Cruz. 2023. Explainable reinforcement learning for broad-xai: a conceptual framework and survey. *Neural Computing and Applications* 35, 23 (2023), 16893–16916.

[11]. S. Kate Devitt and Damian Copeland. 2023. Australia's approach to AI governance in security and defence. In *The AI Wave in Defence Innovation*. Routledge, 217–250.

[12]. Sharma, A., et al. (2023). A novel approach for detection of APT malware using multi-dimensional hybrid Bayesian belief network. *International Journal of Information Security, 22,* 119–135. https://doi.org/10.1007/s10207-022-00631-5

[13]. Vyas, S., Hannay, J., Bolton, A., & Burnap, P. (2023). Automated cyber defence: A review. *Proceedings of the ACM on Measurement and Analysis of Computing Systems, 37*(4), Article 111, 32 pages. https://doi.org/XXXXXXX.XXXXXXX

[14]. Vyas, S., Mavroudis, V., & Burnap, P. (2025). Towards the deployment of realistic autonomous cyber network defence: A systematic review. *ACM Computing Surveys, 58*(1), Article 36, 36 pages. https://doi.org/10.1145/3729213

[15]. Wang, Y., Xing, W., Zhang, J., Liu, L., & Zhao, X. (2024). Remote state estimation under DoS attacks in CPSs with arbitrary tree topology: A Bayesian Stackelberg game approach. *IEEE Transactions on Signal and Information Processing over Networks, 10,* 527–538.

[16]. Waqas, M., et al. (2023). Defense scheme against advanced persistent threats in mobile fog computing security. *Computer Networks, 221,* 109519. https://doi.org/10.1016/j.comnet.2022.109519

[17]. Xuan, C. D., & Dao, H. M. (2021). A novel approach for APT attack detection based on combined deep learning model. *Neural Computing and Applications, 33,* 13251–13264. https://doi.org/10.1007/s00521-021-05952-5

[18]. Xuan, C. D., Duong, D., & Dau, H. X. (2021). A multi-layer approach for advanced persistent threat detection using machine learning based on network traffic. *Journal of Intelligent & Fuzzy Systems, 40,* 11311–11329. https://doi.org/10.3233/JIFS-202465

[19]. Xuan, C. D., & Nguyen, T. T. (2024). A novel approach for APT attack detection based on an advanced computing. *Scientific Reports, 14,* 22223. https://doi.org/10.1038/s41598-024-72957-0

[20]. Xue, D., Chi, Y., Wu, B., & Zhao, L. (2023). APT attack detection scheme based on CK sketch and DNS traffic. *Sensors, 23*(4), 2217. https://doi.org/10.3390/s23042217

[21]. Yang, G., Sun, X., Liu, L., & Li, X. (2022). Cyber attacks on remote state estimation in cyber-physical systems: A game-theoretic approach. In *Advances in applied nonlinear dynamics, vibration and control-2021: Proceedings of the 2021 International Conference on Applied Nonlinear Dynamics, Vibration and Control (ICANDVC2021)* (pp. 1–15). Springer.

[22]. Yi, T., Chen, X., Zhu, Y., Ge, W., & Han, Z. (2023). Review on the application of deep learning in network attack detection. *Journal of Network and Computer Applications, 212,* 103580. https://doi.org/10.1016/j.jnca.2022.103580

[23]. Yu, Y., Liu, G. P., Huang, Y., & Hu, W. (2023). Optimal resilient tracking control for networked systems with multi-channels under attacks. *IEEE Transactions on Industrial Electronics, 71,* 3001–3011.

[24]. Zhang, L., Zhu, T., Hussain, F. K., Ye, D., & Zhou, W. (2023). A game-theoretic method for defending against advanced persistent threats in cyber systems. *IEEE Transactions on Information Forensics and Security, 18,* 1349–1364. https://doi.org/10.1109/TIFS.2022.3229595

[25]. Zhou, J., Shang, J., & Chen, T. (2024). Cybersecurity landscape on remote state estimation: A comprehensive review. *IEEE/CAA Journal of Automatica Sinica, 11,* 851–865.